PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-028116
(43)Date of publication of application : 27.01.1998

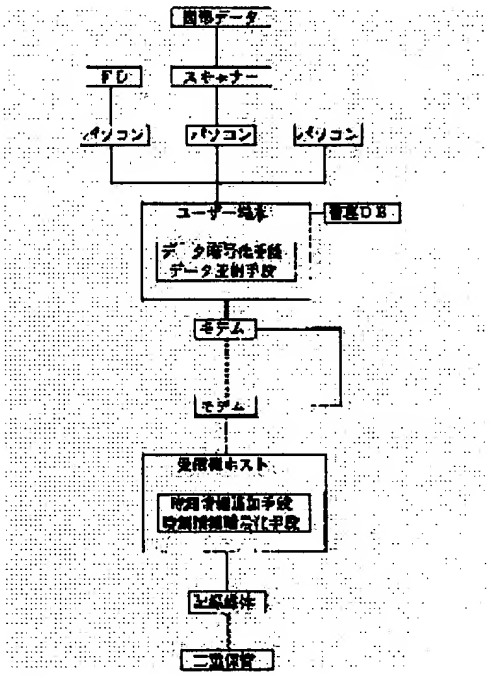
(51)Int.Cl. H04L 9/16
G09C 1/00
G09C 1/00
G09C 1/00
H03M 7/30
H04L 9/08
H04L 9/06
H04L 9/32

(21)Application number : 08-181752
(22)Date of filing : 11.07.1996

(71)Applicant : ARAKI TADASHI
KURODA HIROMICHI
(72)Inventor : ARAKI TADASHI
KURODA HIROMICHI

(54) METHOD FOR RECORDING RECEIVED DATA

(57)Abstract:
PROBLEM TO BE SOLVED: To improve the safety of various kinds of data by recording ciphered transmission data in a recording medium unable for rewriting as time added data where time information is added by means of a time information adding means.
SOLUTION: Time information for a time added data is added to transmission work data in a compressed state by a time information compressing means. When time information is recorded in the recording medium as time data unable for rewriting after ciphering, the state becomes the one where decoding or rewriting is not easily executed since ciphered time information is, moreover, added to ciphered transmission data in a certain plate of time added data even when the data is leaked. A cipher key is required in ciphering time information, a decoding key is required in decoding and the cipher key and the decoding key are provided by a receivern. Thus, a call originator safely trusts data to the receiver.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－28116

(43)公開日　平成10年(1998)１月27日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ			技術表示箇所
Ｈ０４Ｌ	9/16			Ｈ０４Ｌ	9/00	６４３	
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｚ	
		６４０	7259－5Ｊ			６４０Ａ	
			7259－5Ｊ			６４０Ｄ	
			7259－5Ｊ			６４０Ｚ	

審査請求　未請求　請求項の数17　ＯＬ　（全 10 頁）　最終頁に続く

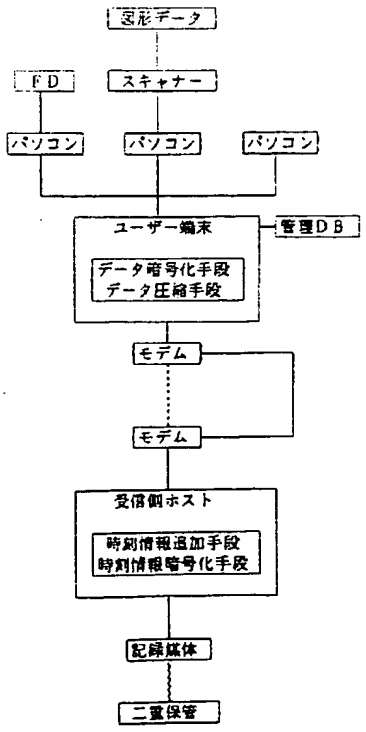
(21)出願番号　特願平8－181752

(22)出願日　平成８年(1996)７月11日

(71)出願人　596018001
荒木　義
東京都港区高輪４丁目14番13号
(74)上記１名の代理人　弁理士　黒田　博道
(71)出願人　595029509
黒田　博道
東京都練馬区貫井１－23－７－201
(74)上記１名の代理人　弁理士　木村　高明　(外２名)
(72)発明者　荒木　義
東京都港区高輪４丁目14番13号
(72)発明者　黒田　博道
東京都練馬区貫井１－23－７－201

(54)【発明の名称】　データの受信記録方法

(57)【要約】
【課題】　日付と共に内容の確定が必要な事項について、極めて簡易な手段により、かつ種々のデータの安全性を考慮しつつ受信記録する。
【解決手段】　データ暗号化手段によって暗号化した送信加工データを、時刻情報追加手段によって時刻情報を追加した時刻加工データとして記録媒体に書き換え不能に記録する。暗号化されない送信データを記録することもできる。



【特許請求の範囲】

【請求項１】　データ暗号化手段によって暗号化した送信加工データを、時刻情報追加手段によって時刻情報を追加した時刻加工データとして記録媒体に書き換え不能に記録することを特徴としたデータの受信記録方法。

【請求項２】　データ暗号化手段によって暗号化した送信加工データと、暗号化されない送信データとを、時刻情報追加手段によって時刻情報を追加した時刻加工データとして記録媒体に書き換え不能に記録することを特徴としたデータの受信記録方法。

【請求項３】　送信加工データがデータ圧縮手段によって圧縮されていることを特徴とした請求項１または２記載のデータの受信記録方法。

【請求項４】　時刻情報圧縮手段によって時刻情報を圧縮して時刻加工データとすることを特徴とした請求項１，２または３記載のデータの受信記録方法。

【請求項５】　時刻情報は受信者が提供することを特徴とした請求項１，２，３または４記載のデータの受信記録方法。

【請求項６】　時刻情報は第三者が提供することを特徴とした請求項１，２，３または４記載のデータの受信記録方法。

【請求項７】　時刻情報追加手段によって、時刻情報を、時刻加工データの前、後、中間のいずれか１以上の部分に追加することを特徴とした請求項１，２，３，４，５または６記載のデータの受信記録方法。

【請求項８】　データ暗号化手段によって暗号化した送信加工データを解読するデータ解読手段を送信者が有していることを特徴とした請求項１，２，３，４，５，６または７記載のデータの受信記録方法

【請求項９】　時刻情報暗号化手段によって時刻情報を暗号化することを特徴とした請求項１，２，３，４，５，６，７または８記載のデータの受信記録方法

【請求項１０】　時刻情報暗号化手段によって暗号化した時刻情報を解読する時刻情報解読手段を第三者または受信者のいずれか一方または双方が有していることを特徴とした請求項９記載のデータの受信記録方法。

【請求項１１】　データ暗号化手段によって行う暗号化を、時刻にしたがって暗号化の手段が変化する時刻変化データ暗号化プログラムにしたがって行うことを特徴とした請求項１，２，３，４，５，６，７，８，９または１０記載のデータの受信記録方法。

【請求項１２】　時刻情報暗号化手段によって行う時刻情報の暗号化を、時刻にしたがって暗号化の手段が変化する時刻変化時刻情報暗号化プログラムにしたがって行うことを特徴とした請求項９，１０または１１記載のデータの受信記録方法。

【請求項１３】　送信加工データと送信データとを別個に書き換え不能に記録することを特徴とした請求項２，３，４，５，６，７，８，９，１０，１１または１２記載のデータの受信記録方法。

【請求項１４】　時刻情報追加手段によって送信加工データに時刻情報を加えた受信データを、受信者から送信者に送信することを特徴とした請求項２，３，４，５，６，７，８，９，１０，１１，１２または１３記載のデータの受信記録方法。

【請求項１５】　時刻情報として少なくとも受信終了時刻を用い、この受信終了時刻情報の時刻情報追加手段による追加終了信号を、書き換え不能な記録の開始信号として利用することを特徴とした請求項１，２，３，４，５，６，７，８，９，１０，１１，１２，１３または１４記載のデータの受信記録方法。

【請求項１６】　時刻加工データを、送信順に記録媒体に書き換え不能に記録することを特徴とした請求項１，２，３，４，５，６，７，８，９，１０，１１，１２，１３，１４または１５記載のデータの受信記録方法。

【請求項１７】　受信者が、時刻加工データの一部又は全部を、更に他の受信者に転送し、複数の受信者が記録媒体に書き換え不能に記録することを特徴とした請求項１，２，３，４，５，６，７，８，９，１０，１１，１２，１３，１４，１５または１６記載のデータの受信記録方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はデータの受信記録方法、更に詳しくは暗号化したデータを受信する際に時刻情報を追加し、更に書き換え不能な状態で記録することによって、送信されたデータの受け取り日時を特定可能としたデータの受信記録方法に関するものである

【０００２】

【従来の技術】従来から、データの作成された日時、あるいは作成後の特定日時にデータが存在していたことを立証することが必要な場合があった。例えば、発明日を認定する場合については、特定の日に発明が完成していたことの立証が必要とされていた。また先使用権を主張するためには、特定の日にはすでに実施していたことを立証ことが必要とされていた。更に、コンピュータプログラムについては、その作成日の立証が必要な場合もあった

【０００３】従来、このような場合には、一般的に、発明が完成していたことを立証できる書類、発明を実施していたことを立証できる書類あるいはコンピュータプログラムリスト等を作成し、それらの書類あるいはリストに公証人からの確定日付を付してもらうことによって、後日日付の立証を可能とすることが行われていた。また発明に関しては、特許庁に出願することによって、少なくとも出願日には発明が完成していたことを立証できることともなっていた。

【０００４】更にコンピュータプログラムに関しては、第１創作年月日登録を行うことによって、コンピュータ

プログラムの創作日の特定が行えるようにもなっていた。

【0005】

【発明が解決しようとする課題】ただこのような各制度の中で、公証人による立証に関しては、複数枚の書類は各書類毎に確定日付を付してもらう必要があり、繁雑な作業となっていた。特に研究者が日々作成する実験データ等に関しては、この公証人による確定日付を付す行為を毎日行うことが現実的に無理なこととなっていた。

【0006】また特許出願に関しても、発明の完成日と特許出願日との間に時間的なずれが生じると共に、発明完成に至る途中の研究結果については、発明として完成していないために、特許出願の対象にできないこととなっていた。更にコンピュータプログラムに関しても、バージョンアップをした場合に、新しい著作物として登録すべきか、あるいは以前のコンピュータプログラムの範囲かが不明な場合が多く、登録に苦慮することともなっていた。

【0007】そこで、本発明は、発明日の立証、研究開発等の進捗状況、実施の立証、コンピュータプログラムの創作等のように、日付と共に内容の確定が必要な事項について、極めて簡易な手段により、かつ種々のデータの安全性を考慮しつつ受信記録する方法を提供することを目的としたものである。

【0008】

【課題を解決するための手段】前述した目的を達成するために、本発明のうちで、請求項1記載の発明は、データ暗号化手段によって暗号化した送信加工データを、時刻情報追加手段によって時刻情報を追加した時刻加工データとして記録媒体に書き換え不能に記録することを特徴とした。

【0009】ここで、暗号化する以前のデータは、文字、数式、図形、写真等の形で表される事象、概念等の内で、計算機プログラムが処理対象とし、データ伝送可能なデータをいう。具体的には、アナログデータ及びディジタルデータを含むものである。そしてこのようなデータの暗号化とは、復元可能な状態で情報を意味のわからない情報に変換することをいう。このデータの暗号化は通常コンピュータを用いた暗号化手段によって行われる。更に暗号化するのは、その後に行うデータ伝送時のデータ漏洩を防止するために行うものである。

【0010】暗号化手段の具体例としては、秘密鍵方式あるいは公開鍵方式を用いることによって、情報を暗号化すること等によって行うことができる。具体的には、暗号鍵を用いて情報を暗号化するものであり、この暗号化された情報は復号鍵を用いて元の情報に復元させることが可能となっている。著名な手段としては、ＤＥＳ等がある。

【0011】送信加工データは、暗号化する以前のデータを暗号化手段によって暗号化したデータをいい、モデムを介して伝送可能となっている。時刻情報とは、年、月、日、時、分、秒等のような、ある瞬間の時刻を特定するための情報をいう。またここにおける時刻情報は、受信者が所用する時計等にしたがって供給することもできるし、データを電送するための機関、例えばＮＴＴが有している時刻を用いることもできるし、更には日本標準時あるいはグリニッジ標準時を用いることもできる。

【0012】ここで時刻情報追加手段とは、送信加工データのいずれかの場所に、時刻情報を追加することをいう。このようなことは、送信加工データを受け入れた時刻を特定するためである。したがって、時刻加工データとしては、送信加工データに時刻情報が追加されたデータとなっている。

【0013】また、書き換え不能に記憶するとは、ディジタルデータあるいはアナログデータを書き換えが不能な記録媒体、あるいは書き換え可能な記録媒体に書き換え不能な状態で記憶させることをいう。具体的には、半導体ディスク、ハードディスク、光ディスク、フロッピーディスク、磁気テープ等に書き換え不能に記憶するものである。光ディスクを例にすると、例えば記録内容を書き換えられないように追記型光ディスクを用いることもできるし、消去、再書き込み可能な光磁気ディスクを用いるものの、この光磁気ディスクへの書き込みのためのハードウェアにおいて、消去、再書き込み不能となるように制御することによって、結果的に、書き換え不能に記憶させることもできる。

【0014】更に、請求項2記載の発明は、データ暗号化手段によって暗号化した送信加工データと、暗号化されない送信データとを、時刻情報追加手段によって時刻情報を追加した時刻加工データとして記録媒体に書き換え不能に記録することを特徴とした。ここで、暗号化されない送信データとは、送信者、送信内容名等からなるデータであって、後日、データを検索する際の目次となるようなデータをいう。このような送信データに関しては、暗号化してしまうことによる検索の不便をさけるため、この請求項に記載された発明では、暗号化しないこととしたものである。もちろん、すべてのデータを暗号化して送信加工データとした後、受信側が、時刻加工データ毎に検索可能なラベルを付しておいて、このラベルによって検索することも可能である。

【0015】さらに、請求項3記載の発明は、請求項1または2記載の発明の構成を備えていると共に、送信加工データがデータ圧縮手段によって圧縮されていることを特徴とした。ここで、データ圧縮手段とは、内容を変更することなくデータ量を減少させるための公知の手段であり、例えばランレングス符号化等の手段をとることができる。

【0016】更にここでは、送信加工データのみならず、送信データをもデータ圧縮手段によって圧縮することで、送信時間等の減縮、及び書き換え不能な状態での

保存データ量の削減を図ることができる。また、請求項4記載の発明は、請求項1，2または3記載の発明の構成を備えていると共に、時刻情報圧縮手段によって時刻情報を圧縮して時刻加工データとすることを特徴とした。

【0017】時刻情報圧縮手段とは、時刻加工データ全体のデータ量を減少させるために行うものであって、前述したようなデータ圧縮手段を用いることができる。請求項5記載の発明は、請求項1，2，3または4記載の発明の構成を備えていると共に、時刻情報は受信者が提供することを特徴とした。ここで、時刻情報を受信者が提供するとは、受信者が時計等の時刻情報提供手段を有しており、その受信者が有している時刻情報提供手段からの時刻情報を送信加工データに追加して時刻加工データとすることをいう。

【0018】請求項6記載の発明は、請求項1，2，3または4記載の発明の構成を備えていると共に、時刻情報は第三者が提供することを特徴とした。ここで第三者とは、送信者及び受信者を除いたものをいう。具体的には、社会的信用を有している機関、例えば銀行、データを電送するための機関、例えばＮＴＴ（登録商標）、更には電波の状態で常に流している日本あるいはグリニッジの標準時の提供者等をいう。

【0019】請求項7記載の発明は、請求項1，2，3，4，5または6記載の発明の構成に加えて、時刻情報追加手段によって、時刻情報を、時刻加工データの前、後、中間のいずれか1以上の部分に追加することを特徴とした。ここで時刻情報追加手段とは、送信加工データあるいは送信加工データ及び送信データに時刻情報を追加して時刻加工データとするための手段である。ここで、どの時刻にデータを受け取ったのかということを記録するためには、時刻加工データの最後尾に時刻情報を追加しておけば足りる。ただこの他にも、データの送信時間が短い場合には最前部に追加することもできるし、場合によっては、データの途中に追加することもできる。このようにデータの途中に追加すると、時刻情報が全データのどこにあるのかということが判明しずらくなるので、時刻情報を含めた安全性が向上する。

【0020】更にはこの時刻データは、送信加工データ等の途中の複数の箇所に挿入することもできる。またこの時、時刻上方を書く秒ごとに挿入することもできる。この場合、いわゆる「電子すかし」の手法を用いることも可能である。また、請求項8記載の発明は、請求項1，2，3，4，5，6または7記載の発明の構成に加えて、データ暗号化手段によって暗号化した送信加工データを解読するデータ解読手段を送信者が有していることを特徴とした。

【0021】ここでデータ解読は、復号鍵によって行うものである。データの暗号化に関しては、一般には発信者が暗号鍵を持ち、受信者が復号鍵を持つことによって、暗号鍵によって暗号化した情報を発信者が受信者に送り、受信者が受信後に復号鍵によって解読して読むことができるようになっていた。ただ、請求項8記載の発明では、発信者が暗号鍵と復号鍵とを有しており、発信者が暗号化した情報は発信者以外の人では解読できないようになっている。このようにすることで、発信者が有している情報が他に漏れることを防止するものである。なおここで、暗号鍵と復号鍵とは同一のものを使うことができるが、異なった鍵を用いることもできる。

【0022】なお、ここにおける復号鍵については、二重鍵として、発信者の復号鍵と、受信者あるいは第三者が有する復号鍵とを同時に使用した場合に限って、解読することができるようにすることもできる。なおここで、暗号鍵あるいは復号鍵は、発信者が選択することもできるが、受信者が選択し、発信者が使用するようにすると、発信者が書き換えたりすることが不能なことから、送信加工データの信頼性が更に向上する。

【0023】請求項9に記載の発明は、請求項1，2，3，4，5，6，7または8記載の発明の構成に加えて、時刻情報暗号化手段によって時刻情報を暗号化することを特徴とした。このように時刻情報をも暗号化した時刻加工データとして記録媒体に書き換え不能に記録すると、万一、時刻加工データが漏洩した場合であっても、暗号化した送信加工データに、更に暗号化した時刻情報が、時刻加工データのいずれかの場所に追加されることとなるので、極めて解読が行いにくい状態となる。

【0024】請求項10に記載の発明は、請求項9記載の発明の構成に加えて、時刻情報暗号化手段によって暗号化した時刻情報を解読する時刻情報管理手段を第三者または受信者の一方または双方が有していることを特徴とした。ここで、時刻情報を暗号化する際にも、暗号鍵が必要であり、更に解読する際には復号鍵が必要とされる。ここで、復号鍵に関しては、受信者が有しており、必要に応じて時刻情報を解読することを可能とすることもできる。一方、この時刻情報に関する復号鍵を発信者あるいは受信者以外の第三者が有しているように形成することもできる。このようにすると、受信者は、送信加工データのみならず、時刻情報も、一旦記録媒体に書き換え不能に記録した後は、いっさい内容にアクセスすることができなくなる。したがって、受信者からのデータの解読あるいは書き換えが不能となるので、発信者は情報を預ける受信者に対して、安心してデータを預けることができるものである。

【0025】請求項11に記載の発明は、請求項1，2，3，4，5，6，7，8，9または10記載の発明の構成に加えて、データ暗号化手段によって行う暗号化を、時刻にしたがって暗号化の手段が変化する時刻変化データ暗号化プログラムにしたがって行うことを特徴とした。データの暗号化に関しては、種々の手法がある。そのような手法の一として、前述したようなＤＥＳもあ

げられる。

【００２６】ここで請求項１１に記載した発明のように、暗号化を時刻にしたがって暗号化の手段が変化する時刻変化データ暗号化プログラムにしたがって行うと、暗号化したものを解読することが極めて困難となる。具体的には、複数の暗号化プログラムと、その複数の暗号化プログラムの適用順序と、その適用順序を時刻にしたがって決定する手段とを有する暗号鍵を用意して、暗号化するような場合が考えられる。

【００２７】極めて簡単な例を挙げると、暗号化プログラムとしてＡＢＣＤＥＦの６通りを用意する。この暗号化プログラムの適用順序としてＡＢＣＤＥＦの組み合わせで７２０通りの順序がある。この組み合わせを２４時間で振り分けると、各時間当たり３０通りの適用順序が与えられる。

【００２８】そして、暗号化を開始するときの適用プログラム及びその後の適用順序を２分単位で定めておく。単純にこれだけを組み合わせれば、暗号化の開始時の適用プログラム及びその後の適用順序が定まっているので、その後は例えば１秒単位で適用順序をあらかじめ定められた順序で変更することによって、１秒単位で暗号化するためのプログラムが変化することとなる。

【００２９】このように形成することによって、データの解読がより困難となり、データの秘密性が向上する。もちろんここで、あらかじめ用意する暗号化プログラムの数を増減させたり、あるいは適用順序の変更のための時間を変更したりすることができる。請求項１２に記載の発明は、請求項９，１０または１１記載の発明の構成に加えて、時刻情報暗号化手段によって行う時刻情報の暗号化を、時刻にしたがって暗号化の手段が変化する時刻変化時刻情報暗号化プログラムにしたがって行うことを特徴とした

【００３０】ここで用いられる時刻変化時刻情報暗号化プログラムは、前述した時刻変化データ暗号化プログラムと同様に用いることができる。このように形成することによって、時刻データの解読がより困難となり、データ全体の秘密性が向上する。請求項１３に記載の発明は、請求項２，３，４，５，６，７，８，９，１０，１１または１２記載の発明の構成に加えて、送信加工データと送信データとを別個に書き換え不能に記録することを特徴とした。

【００３１】このように形成することによって、送信加工データは暗号化され、送信データは暗号化されないままで書き換え不能に記録されるので、暗号化されない送信データの検索を行うことによって、データリストを作ったり、あるいは呼出を行ったりすることが容易となる。更にこの場合であっても、送信加工データは暗号化されているので、データの秘密性は担保できるものである。

【００３２】請求項１４に記載の発明は、請求項２，３，４，５，６，７，８，９，１０，１１，１２または１３記載の発明の構成に加えて、時刻情報追加手段によって送信加工データに時刻情報を加えた受信データを、受信者から送信者に送信することを特徴とした。このようにすることで、受信者が、確実に受信したということと、いつ受信したのかということを発信者が確認できるものである。

【００３３】またこの際、受信者から発信者に送り返すデータは、送信加工データと時刻情報とからなっているために、データの秘密性は担保されている。請求項１５に記載の発明は、請求項１，２，３，４，５，６，７，８，９，１０，１１，１２，１３または１４記載の発明の構成に加えて、時刻情報として少なくとも受信終了時刻を用い、この受信終了時刻情報の時刻情報追加手段による追加終了信号を、書き換え不能な記録の開始信号として利用することを特徴とした。

【００３４】ここで、本願発明は、時刻加工データを記録媒体に書き換え不能に記録するものである。ここで、その記録を開始するためのトリガーとしては、例えば時刻加工データとした後にマニュアルの操作によって記録することもできる。ただ請求項１５に記載した発明のように、受信終了時刻情報の時刻情報追加手段による追加終了信号を、書き換え不能な記録の開始信号として利用すれば、受信終了と同時に時刻情報を書き込んで記録できることとなる。

【００３５】請求項１６記載の発明は、請求項１，２，３，４，５，６，７，８，９，１０，１１，１２，１３，１４または１５記載の発明の構成に加えて、時刻加工データを、送信順に記録媒体に書き換え不能に記録することを特徴とした。このようにすると、複数回あるいは複数社から送信されたデータが、順次記録されることとなる。したがって、ある特定の時刻加工データに関する時刻情報の信頼性に関しては、前後の時刻加工データからも特定されることとなるので、一層向上することとなる。

【００３６】請求項１７記載の発明は、請求項１，２，３，４，５，６，７，８，９，１０，１１，１２，１３，１４，１５または１６記載の発明の構成に加えて、受信者が、時刻加工データの一部又は全部を、更に他の受信者に転送し、複数の受信者が記録媒体に書き換え不能に記録することを特徴とした。このように、複数の受信者を用意し、各々の受信者が記録することとすれば、地震等の災害があったとしても、記録が破壊される虞が少ない。更にここで、他の受信者を、外国、例えば弁国におくと、日本の受信者が受信すると同時に、米国においても先発明等との関係で必要なデータのみを転送記録しておくことが可能となる。

【００３７】

【発明の実施の形態】以下、本発明の実施の形態を、本発明に係わるデータの受信記録方法を用いたデータの送

受信記録方法の説明と共に、図事例にしたがって説明する。図１は、データの送受信記録方法を説明するための概略図である。この図においては、発信者が、パソコンを用いて種々のデータを作り、そのデータをユーザー端末を用いて受信側ホストに送信し、受信側では受信した情報を記録媒体に記録するものである。

【００３８】ここで種々のデータを作るパソコンは、パソコンで直接データを打ち込むこともあるし、図形、写真、図面、グラフ等の図形データをスキャナーを介することによってイメージデータとした後に、あるいはディジタルカメラ等から直接イメージデータとした後にパソコンに取り込むこともあるし、更には、ＦＤ等の外部記憶媒体に格納したデータをパソコンで読み込んでデータとすることもある。

【００３９】いずれの場合であっても、パソコンを介したデータは、文字、数式、図形、動画、写真等の形で表される事象、概念等の内で、計算機プログラムが処理対象とし、パソコン処理の後にデータ伝送可能なデータをいう。具体的には、アナログデータ及びディジタルデータを含むものである。またここで、パソコンを介するとして説明したが、ユーザー端末にパソコンの機能を備えさせ、ユーザー端末で直接処理することもできる。

【００４０】具体的に、ここでのデータとしては、発明の完成、先発明あるいは先使用による通常実施権取得のためのデータとして、開発記録、実験データ、設計図面、特許の提案書、工場内レイアウト、実施を示す写真等があげられる。また、トレードシークレックの保護のためのデータとして、従業員の入社時の秘密保持誓約書、開発段階での秘密保持誓約書、トレードシークレット特定のための資料、秘密管理を行っていることを証する資料、トレードシークレット自体等があげられる。ここでデータとして秘密保持契約における関連書類をあげると、この契約における秘密情報を特定するための資料、あるいは契約前公知事項の確認のための資料等があげられる。またＰＬ関係のデータとしては、開発段階あるいは製造段階での安全性確認のための実験データ、商品販売前に行う権威者による安全確認の証明、製造工程中の安全確認のデータ、使用説明書作成のためのデータ等があげられる。また通常の契約書に関しても、ここでいうデータとして用いられるだけでなく、契約当事者の署名あるいは捺印がある契約書をここでいうデータとして扱うと、契約書の第三者への寄託ともなる。更には、コンピュータプログラムをデータとして考えると、著作物の成立過程の記録が行えるだけでなく、ソフトウェアエスクロウ制度の下でのソースコードの寄託先としても利用できる。なお、もちろんのことであるが、前記したデータ以外にも、種々のデータをここでいうデータに含めることができる。

【００４１】このようなデータは、一旦ユーザー端末に入力される。もちろん、前記したパソコンを直接ユーザー端末として使用することも可能である。またここにおけるユーザー端末は、データ圧縮手段とデータ暗号化手段とを備えているものである。ここで、データ圧縮手段とは、内容を変更することなくデータ量を減少させるための公知の手段であり、例えばランレングス符号化等の手段をとることができる。

【００４２】ここで、データの暗号化とは、情報を意味のわからない情報に変換することをいう。このデータの暗号化は通常コンピュータを用いた暗号化手段によって行われる。更に暗号化するのは、その後に行うデータ伝送時のデータ漏洩を防止するために行うものである。更に、データ暗号化手段の具体例としては、秘密鍵方式あるいは公開鍵方式を用いることによって、情報を暗号化すること等によって行うことができる。具体的には、暗号鍵を用いて情報を暗号化するものであり、この暗号化された情報は復号鍵を用いて元の情報に復元させることが可能となっている。著名な手段としては、ＤＥＳ等がある。

【００４３】ここにおけるデータの暗号化に関して、手段を問うものではないが、時刻にしたがって暗号化の手段が変化する時刻変化データ暗号化プログラムにしたがって行うと、暗号化したものを解読することが極めて困難となる。具体的には、複数の暗号化プログラムと、その複数の暗号化プログラムの適用順序と、その適用順序を時刻にしたがって決定する手段とを有する暗号鍵を用意して、暗号化するような場合が考えられる。

【００４４】ここでは、暗号化プログラムとしてＡＢＣＤＥＦＧＨＩの９通りの暗号化手段が用意してある。この暗号化プログラムの適用順序として、ＡＢＣＤＥＦＧＨＩから始まって、ＡＢＣＤＥＦＧＩＨ……ＩＨＧＦＥＤＣＢＡまでの組み合わせが３６２８８０通りとなる。まず最初に、この組み合わせの中で、８６１００通りの組み合わせを選択し、次いでその順序までをも暗号鍵毎に定めている。

【００４５】そして、この組み合わせを２４時間で振り分けると、各秒あたり１通りの適用順序が与えられる。すると、暗号化の開始時間によって、それぞれ異なった組み合わせの暗号化プログラムが適用されることとなる。また更に、時刻によって組み合わせが特定された暗号化プログラム中の各暗号化プログラムは、０．２秒たつと次の暗号化プログラムに移行することとしてある。そして、時刻によって特定された組み合わせの暗号化プログラムにしたがって、順次８通りの暗号化プログラムが１．８秒間で終了すると、次いでそのときの時刻が確認され、その時刻にあった次の組み合わせの暗号化プログラムが適用されることとなる。

【００４６】具体的には、ある時刻、例えば午後４時１２分１８秒の時刻に暗号化を開始したとする。この時の暗号化プログラムの順序が例えばＢＨＩＡＦＣＥＤＧの組み合わせであったとすると、最初に、Ｂの暗号化プロ

グラムで、０．２秒間だけ暗号化され、次ぎにＨの暗号化プログラムで０．２秒間だけ暗号化され、以下順次繰り返すことによって、１．８秒間で、ある時刻の暗号化プログラムにしたがって暗号化が行われる。この時点で前データすべての暗号化が行われていない場合には、次いで午後４時１２分１９秒の時刻の暗号化プログラムである、例えばＧＡＦＨＣＥＢＩＤの組み合わせで暗号化が行われる。そして１．８秒経過後は、今度は午後４時１２分２１秒の時刻の暗号化プログラムで暗号化が行われるものである。

【００４７】このように形成することによって、データの解読がより困難となり、データの秘密性が向上する。もちろんここで、あらかじめ用意する暗号化プログラムの数を増減させたり、あるいは適用順序の変更のための時間を変更したりすることができる。このようにデータ圧縮手段あるいはデータ暗号化手段によってデータの圧縮あるいは暗号化が行われた後、モデムを介してデータが発信されることとなる。

【００４８】更にこの時、データをそのまま、あるいはデータ圧縮手段によって圧縮をかけた後、更には必要に応じてデータ暗号化手段によって暗号化した後、ユーザーが有している管理データベースに記録することも可能である。このようにすることによって、ユーザーが自己の社内等で、データを使用することが可能となるものである。

【００４９】更に、モデムを介してデータを送信する際に、暗号化されない送信データをつける場合がある。このような送信データとしては、例えば送り状ナンバー、企業コード、事業所（研究所）コード、テーマコード、個人コード、送信日、キーワード等を用いている。ここで、企業コード、事業所（研究所）コード、テーマコード、個人コードによって、どの会社のどの事業所（研究所）でいるどのようなテーマの研究であり、かつ誰が作ったデータであるのかということのインデックスにすることができる。更にこの中で、事業所（研究所）コード、テーマコード、個人コードの設定によって、前記した管理データベースの運用が容易に行えるものである。またキーワードを付加しておくと、検索が容易となる。またここでは、研究者からのデータを対象として説明したが、営業担当者等についても、暗号化するためのデータとして品目コード、数量コード、販売先コード等を設定し、暗号化しない送信データとして営業所コード、セクションコード、個人コード等を設定しておけば、送信したデータ確認が容易に行えるだけでなく、前記した管理データベースの運用によって営業管理が容易に行えるものである。

【００５０】またこのような暗号化されない送信データは、受信側の保管リストとして用いることもできる。なお、このような送信データに関しては、いっさい添付しないこともできる。その場合には、受信側で受信した後に、返送する受領確認書の番号で暗号化したデータの確認を行うものである。

【００５１】モデムを介してのデータの送信は、一般のアナログ電話回線あるいはＩＳＤＮのようなディジタル電話回線を用いて行える。受信側では、やはりモデムを介して受信する。その後、受信側ホストコンピュータに入力される。この入力段階で、受信側ホストコンピュータに入力されるデータには、データ暗号化手段によって暗号化された送信加工データ及び暗号化されない送信データが含まれている。ただ少なくともここで、受信側ホストコンピュータに入力されるデータのうちで、秘密状態に維持したいデータに関しては、予め暗号化手段によって暗号化されているので、受信側で送信されたデータの内容を理解することはできない。

【００５２】なおこのようにして送信されたデータは、時刻情報追加手段を用いて、時刻情報を追加して時刻加工データとする。ここで時刻情報とは、年、月、日、時、分、秒等のような、ある瞬間の時刻を特定するための情報をいう。またここにおける時刻情報は、受信者が所有する時計に表示される時刻を入力するものである。

【００５３】ただこの他にも、社会的信用を備えている機関、例えば銀行等が有している時刻を用いたり、データを電送するための機関、例えばＮＴＴが有している時刻を用いたり、電波の形でながされている日本標準時あるいはグリニッジ標準時を用いることもできる。またここで、時刻情報追加手段とは、送信加工データのいずれかの場所に、時刻情報を追加することをいう。

【００５４】また時刻情報を追加する場所については、送信加工データの、前、中間、後の何れの場所に行うことも可能である。ただこの実施の形態では、送信加工データのすべてを受信した時刻を、送信加工データの後に追加して時刻加工データとするものである。このようにすることで、少なくともどの時刻に全データが存在していたのかということが明確化できるものである。もちろんこのときに、送信加工データのすべてを受信した時刻を、送信加工データの前に追加して時刻加工データとすることもできる。

【００５５】もちろんここで、データの送信時間が短かったり、あるいは若干の時刻のズレが余り問題とされない時等には、送信の開始時間を入力することもできる。更に、時刻情報に関しては、送信加工データの前、後の他に、任意の中間に追加することもできる。このようにデータの途中に時刻情報を追加すると、時刻情報が全データのどこにあるのかということが判明しずらくなるので、時刻情報を含めた安全性が向上する。

【００５６】更にはこの時刻データは、送信加工データ等の途中の複数の箇所に挿入することもできる。またこの時、時刻上方を書く秒ごとに挿入することもできる。この場合、いわゆる「電子すかし」の手法を用いることも可能である。なおここで、この実施の形態では、時刻

加工データとするための時刻情報を、時刻情報圧縮手段によって圧縮した状態で送信加工データに追加している。もちろん圧縮しないままで追加することもできるが、圧縮すると記録媒体に保管するデータ量を減少させることができる。

【００５７】更に、この実施の形態では時刻情報を、前述したように時刻情報圧縮手段によって圧縮するに際して、あらかじめ時刻情報暗号化手段によって暗号化した時刻情報を用いることもできる。このように時刻情報を暗号化した上で、時刻加工データとして記録媒体に書き換え不能に記録すると、万一、時刻加工データが漏洩した場合であっても、暗号化した送信加工データに、更に暗号化した時刻情報が、時刻加工データのいずれかの場所に追加されることとなるので、極めて解読あるいは書き換えが行いにくい状態となる。

【００５８】もちろんこのような時刻情報暗号化手段を用いることなく、そのままの時刻情報を追加することも可能である。ここで、時刻情報を暗号化する際には、暗号鍵が必要であり、更に解読する際には復号鍵が必要とされる。この実施の形態では、暗号鍵も復号鍵も、共に受信者が有しており、必要に応じて時刻情報を解読することを可能としてある。このように復号鍵を受信者が保有するようにすることで、受信者が、暗号化した時刻情報を解読した後の時刻加工データを発信者に提供することができる。

【００５９】一方、この時刻情報に関する復号鍵を発信者あるいは受信者以外の第三者が有しているように形成することもできる。このようにすると、受信者は、送信加工データのみならず、時刻情報も、一旦記録媒体に書き換え不能に記録した後は、いっさい内容を知ることができなくなる。したがって、受信者からのデータ漏洩あるいは書き換えが行えなくなるので、発信者は情報を預ける受信者に対して、安心してデータを預けることができるものである。

【００６０】このようにして、送信加工データに時刻情報を追加して時刻加工データとした後は、この時刻加工データを記録媒体に書き換え不能に記録するものである。ここで、この実施の形態では、記録媒体として追記型の光ディスクを用いているものである。また書き換え不能に記録するとは、ライトワンスの状態での記録をいい、読み出すことは可能であるものの、書き換えることあるいは重ね書きすることができないような記録状態をいう。このように書き換え不能に記録するためには、この実施の形態のように、記録媒体自体を書き換え不能なものにすることもできる。ただこの他にも、書き換え可能な記録端体に書き換え不能な状態で記憶させることもできる。具体的には、消去、再書き込み可能な光磁気ディスクを用いるものの、この光磁気ディスクへの書き込みのためのハードウェアを、消去、再書き込み不能となるように制御することによって、結果的に、書き換え不能に記憶させることもできる。またこの実施の形態では記録媒体として光ディスクを用いたが、半導体ディスク、ハードディスク、フロッピーディスク、磁気テープ等であっても、書き換え不能に記録できれば足りる。

【００６１】なお、書き換え不能な記録媒体への記録開始は、例えば時刻加工データとした後にマニュアルの操作によって記録することもできるし、時刻加工データ処理の終了等によって行うこともできる。ただ、受信終了時刻情報の時刻情報追加手段による追加終了信号を、書き換え不能な記録の開始信号として利用すれば、受信終了と同時に時刻情報を書き込んで記録できることとなる。

【００６２】さらにこのように、書き換え不能に記録された時刻加工データは、２組作っておき、相互に距離的に離れた場所に保管しておくと、地震等の災害があった場合でも確実に保管することができる。なおこのように記録媒体に保管された時刻加工データは、暗号化された送信加工データと暗号化された時刻情報とからなる時刻加工データであるので、仮に記録媒体が外部に流出したとしても、内部のデータを読みとることが困難である。またこの際、時刻情報が時刻情報暗号化手段によって暗号化されていない場合にあっても、暗号化された送信加工データを読み取ることができないので、非常事態における安全性も担保できる。

【００６３】また、送信された送信加工データが、すでに暗号化されているので、受信側の人間もそのデータの内容を知ることができない。次にこのデータの秘密管理性を説明するために、データの暗号化に際して用いる鍵について説明する。またここで、この実施の形態における暗号化は、データ暗号化手段によって行うデータの暗号化と、時刻情報暗号化手段によって行う時刻情報の暗号化とがある。

【００６４】そこでまず、データ暗号化手段によって行われるデータの暗号化について説明する。データの暗号化は、暗号鍵によって行うものである。更に、このようにして暗号化したデータの解読は、復号鍵によって行うものである。ここで一般のデータ通信等におけるデータの暗号化に関しては、一般には発信者が暗号鍵を持ち、受信者が受信鍵を持つことによって、暗号鍵によって暗号化した情報を発信者が受信者に送り、受信者が受信後に復号鍵によって解読して読むことができるようになっていた。このようにすることによって通信過程途中でのデータの漏洩を防止するものである。

【００６５】ただ、この実施の形態においては、発信者が暗号鍵と復号鍵とを有しており、発信者が暗号化した情報は発信者以外の人が解読できないようになっている。このようなすることによって、通信の途中であろうが、受信者が受信しているとき、あるいは記録媒体に記録した後のいずれの時であっても、発信者以外はデータの解読が行えないこととなるので、いずれの時点におい

てもデータの漏洩が防止できることとなっている。なおここで、受信者が保有する暗号鍵と復号鍵とは同一のものを使うこともできるが、異なった鍵を用いることもできる。

【００６６】また更に、ここにおける復号鍵については、二重鍵として、発信者の復号鍵と、受信者あるいは第三者が有する復号鍵とを同時に使用した場合に限って、解読することができるようにすることもできる。このようにすることで、記録媒体に記録した後のデータの安全性が更に担保される。なおここで、暗号鍵あるいは復号鍵は、発信者が選択することもできるが、受信者が選択し、発信者が使用するようにすると、発信者が書き換えたりすることが不能なことから、送信加工データの信頼性が更に向上する。

【００６７】一方、時刻情報を暗号化する際にも、暗号鍵が必要であり、更に解読する際には復号鍵が必要とされる。この実施の形態では、暗号鍵及び復号鍵を共に受信者が有しているものである。したがって、受信者が、必要に応じて時刻情報を解読することが可能となっている。一方、この時刻情報に関する復号鍵を発信者あるいは受信者以外の第三者が有しているように形成することもできる。

【００６８】このようにすると、受信者は、送信加工データのみならず、時刻情報も、一旦記録媒体に書き換え不能に記録した後は、時刻情報を含めていっさい内容にアクセスすることができなくなる。したがって、記録媒体を通じてのデータ漏洩あるいは書き換えがなくなるので、発信者は情報を預ける受信者に対して、安心してデータを預けることができるものである。

【００６９】次に、このように記録媒体に保管された時刻加工データを読み出す作業について説明する。まず最初に、発信者がデータの内容の開示を求めるアクションを提起する。このアクションの提起としては、発信者自身の都合による開示の他に、先使用の立証あるいは先使用に基づく通常実施権の立証等における裁判所等からの提出命令にしたがった開示等が考えられる。

【００７０】このような開示を求めるアクションを受けて、受信者が、記録媒体に記録されている時刻加工データを提供するものである。ここで提供される時刻加工データは、送信加工データに暗号化した時刻情報を追加した状態のものと、送信加工データに暗号化していない時刻情報を追加したものとが考えられる。更に後者については、時刻加工データとしては暗号化した時刻情報を追加してあるが、復号鍵によって時刻情報のみを解読したものと、時刻情報を暗号化しないままで追加した時刻加工データとがある。

【００７１】いずれにしても、発信者が自己の都合によってデータの開示を求める場合には、暗号化していない時刻情報を追加した時刻加工データを受信者に提供することが望ましい。一方、裁判所等からの提出命令に対しては、時刻情報を暗号化した時刻加工データをそのまま提出し、時刻情報及び原データの解読のいずれもが裁判手続の中で行われるようにすることで、記録媒体の信頼性をアピールすることができる。

【００７２】なおここで、記録媒体への記録は発信者ごとの記録媒体を用意し、各々の記録媒体に記録することも考えられる。ただ、時刻加工データを、送信順に記録媒体に書き換え不能に記録することを特徴とした。このようにすると、複数個所あるいは複数社から送信されたデータが、順次記録されることとなる。したがって、ある特定の時刻加工データに関する時刻情報の信頼性に関しては、前後の時刻加工データからも特定されることとなるので、一層向上することとなる。

【００７３】更に、前述した説明では、記録媒体に記録させた後に、その記録媒体を他の場所に保管することができるとして説明した。ただ、受信者が、時刻加工データの一部又は全部を、更に他の受信者に転送し、複数の受信者が記録媒体に書き換え不能に記録することを特徴とした。このように、複数の受信者を用意し、各々の受信者が記録することとすれば、地震等の災害があったとしても、記録が破壊される虞が少ない。更にここで、他の受信者を、外国、例えば弁国におくと、日本の受信者が受信すると同時に、米国においても先発明等との関係で必要なデータのみを転送記録しておくことが可能となる。

【００７４】なおこのような発明は、内容証明郵便において、郵便局での保管分をデータとして保管しておくことにも応用できる。このような場合であっても、暗号化された情報の送信となるので、郵便内容の秘密保持は行えるものである。

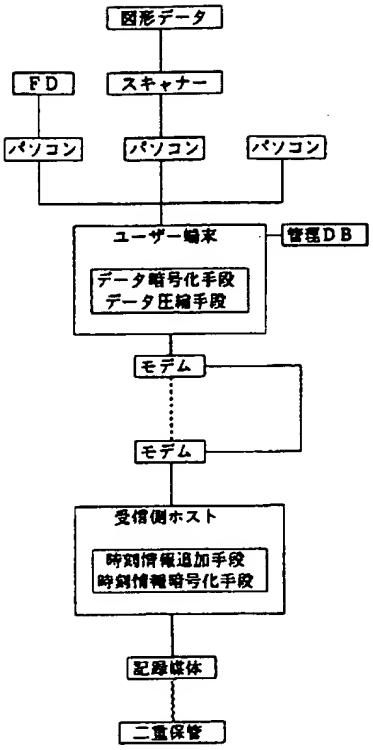
【００７５】

【発明の効果】以上説明したように、本発明は、発明日の立証、研究開発等の進捗状況、実施の立証、コンピュータプログラムの創作等のように、日付と共に内容の確定が必要な事項について、極めて簡易な手段により、かつ種々のデータの安全性を考慮しつつ受信記録することができるものである。

【図面の簡単な説明】

【図１】データの送受信記録方法を説明するための概略図である。

【図１】



フロントページの続き

(51)Int.Cl.⁶		識別記号	庁内整理番号	FI		技術表示箇所
G09C	1/00	660	7259-5J	G09C	1/00	660D
H03M	7/30		9382-5K	H03M	7/30	Z
H04L	9/08			H04L	9/00	601Z
	9/06					611A
	9/32					675A